The opinion in support of the decision being entered today is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD PAUL TARQUINI
AND GEORGE SIMON GALES

Appeal 2007-1276
Application 10/001,446[1]
Technology Center 2100

Decided: July 30, 2007

Before ALLEN R. MACDONALD, JAY P. LUCAS,
and SCOTT R. BOALICK, *Administrative Patent Judges*.

BOALICK, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-10, all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

---

[1] Application filed October 31, 2001. The real party in interest is Hewlett-Packard Development Company, L.P.

STATEMENT OF THE CASE

Appellants' invention relates to a technique for distributing security updates to selected nodes on a network with an Intrusion Protection System (IPS). (Specification 1:7-8.) In the words of the Appellants:

> With reference to FIGURE 7, there is illustrated a logical grouping of nodes disposed in network 200 that facilitates multicasting of command and security updates from management node 85 according to an embodiment of the invention. Web servers 201A-202T may be logically associated by management node 85 based upon the commonality of the services respectively provided thereby. Accordingly, an identification of the logical assignment grouping web servers 201A-201T may be assigned and shared among web servers 201A-202T such that command and security updates, such as attack signatures defining signatures of attacks that may be directed towards a web-content server, may be commonly addressed and distributed only to those nodes that may be effected thereby, i.e., the identification of the logical assignment serves to group one or more nodes of network 200 into logical groups - each node in a group being commonly vulnerable to a particular exploit. In an exemplary embodiment, the identification is preferably implemented as an IP multicast group ID.

(Specification 18:19-32.)

Claim 1 is exemplary:

> 1. A network having an intrusion protection system, comprising:
>
> a network medium;
>
> a management node connected to the network medium and running an intrusion prevention system management application; and
>
> a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Holloway	5,905,859	May 18, 1999

Claims 1-10 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Holloway.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Briefs and the Answer for their respective details. Only those arguments actually made by Appellants have been considered in this decision. Arguments which Appellants could have made but chose not

to make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2004).[2]

ISSUE

The issue is whether Appellants have shown that the Examiner erred in rejecting the claims under 35 U.S.C. § 102(b). The issue turns on whether Holloway teaches or suggests each and every limitation of the claims.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Holloway describes a computer network security system to detect and prevent intrusion into a Local Area Network (LAN) by an unauthorized user. (Col. 1, ll. 14-17.) In particular, Holloway teaches the use of a managed hub to detect and prevent intrusions. (Col. 2, ll. 53-55.) The network has multiple managed hubs. (Col. 4, ll. 51-55.)

2. The system of Holloway transmits a series of frames between the interconnect devices of the network during different phases of its operation. (Col. 2, ll. 58-60.) The frames are sent to a "LAN security

[2] Except as will be noted in this opinion, Appellants have not presented any substantive arguments directed separately to the patentability of the dependent claims or related claims in each group. In the absence of a separate argument with respect to those claims, they stand or fall with the representative independent claim. *See* 37 C.F.R. § 41.37(c)(1)(vii).

feature group address" that is reserved for LAN security features. (Col. 2, ll. 60-65.)

3. In a discovery phase, the managed hub of Holloway determines the interconnect devices (such as switches, bridges, and routers) in the network that are capable of supporting the LAN security feature and builds a table of those interconnect devices. (Col. 2, l. 66 to col. 3, l. 4; col. 3, ll. 25-28.) The managed hub maintains a list of authorized Media Access Control (MAC) addresses for each of its ports. (Col. 3, ll. 4-6.) In a detection phase, the managed hub compares the MAC addresses on each port against the list of authorized MAC addresses in order to detect a security breach. (Col. 3, ll. 34-36.) The code to implement the discovery and detection phases runs within the managed hub. (Col. 9, ll. 33-36; col. 11, ll. 30-32.)

4. If the managed hub detects an unauthorized station connecting to the LAN, it disables the port and transmits a "security breach detected frame" to the LAN security feature group address. (Col. 3, ll. 6-9, 36-40.) When a LAN interconnection device receives the security breach detected frame, it sets up a filter for the intruding MAC address and forwards the security breach detected frame to other LAN segments attached to the interconnection device. (Col. 3, ll. 9-17, 42-49.)

5. Holloway teaches that a network management station can monitor the progress of the security breach detected frame though information that it receives in "trap frames" from the managed hub and the

interconnect devices. (Col. 6, ll. 1-3; col. 15, ll. 27-47; Fig. 17.) The network management station includes a processor and a system bus to which, among other things, RAM, storage devices, and other peripherals are connected. (Col. 5, ll. 10-16; Fig. 3.)

PRINCIPLES OF LAW

On appeal, all timely filed evidence and properly presented argument is considered by the Board. *See In re Piasecki*, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984).

In the examination of a patent application, the Examiner bears the initial burden of showing a prima facie case of unpatentability. *Id.* When that burden is met, the burden then shifts to the applicant to rebut. *Id.*; *see also In re Harris*, 409 F.3d 1339, 1343-44, 74 USPQ2d 1951, 1954 (Fed. Cir. 2005) (finding rebuttal evidence unpersuasive). If the applicant produces rebuttal evidence of adequate weight, the prima facie case of unpatentability is dissipated. *In re Piasecki*, 745 F.2d at 1472, 223 USPQ at 788. Thereafter, patentability is determined in view of the entire record. *Id.* However, on appeal to the Board it is an appellant's burden to establish that the Examiner did not sustain the necessary burden and to show that the Examiner erred -- on appeal we will not start with a presumption that the Examiner is wrong.

Anticipation is established when a single prior art reference discloses expressly or under the principles of inherency each and every limitation of the claimed invention. *Atlas Powder Co. v. IRECO Inc.*, 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1946 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1478-79, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994).

During examination of patent application, a claim is given its broadest reasonable construction consistent with the specification. *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969). "[T]he words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312, 75 USPQ2d 1321, 1326 (Fed. Cir. 2005) (en banc) (internal citations omitted). The "ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313, 75 USPQ2d at 1326.

ANALYSIS

Appellants contend that Examiner erred in rejecting claims 1-10 as being anticipated by Holloway. Reviewing the findings of facts cited above, we do not agree that the Examiner erred in rejecting claims 1-7. In particular, we find that the Appellants have not shown that the Examiner failed to make a prima facie showing of anticipation with respect to claims 1-7. Appellants failed to meet the burden of overcoming that prima facie showing. However, we agree with Appellants that the Examiner erred in rejecting claims 8-10 as being anticipated by Holloway.

Regarding claim 1, Appellants first argue that Holloway does not teach or suggest "a management node connected to the network medium and running an intrusion prevention system management application," as claimed. (Br. 4-5.)

As the Examiner correctly found, the network management station of Holloway meets the "management node" claim limitation. (Answer 3, 6;

FF 5.) We also agree with the Examiner that the network management station inherently runs an intrusion prevention management application in order to perform its monitoring function. (Answer 3, 6; FF 5.) Thus, Holloway teaches a management node connected to the network medium and running an intrusion prevention system management application, as claimed.

Appellants next argue that Holloway does not teach or suggest "a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit," as claimed. (Br. 5-6; Reply Br. 3-4.)

The Examiner found that the managed hubs of Holloway meet the recited "plurality of nodes" limitation, where each managed hub is a node and the MAC address is the identification. (Answer 3, 6.) Appellants assert that the managed hubs cannot meet the "plurality of nodes" limitation because the managed hubs are not grouped together. (Br. 6; Reply Br. 3.) Appellants admit that "the MAC address provides an identification of a computer," but contend that "*Holloway* does not teach that nodes sharing such an identification (i.e., sharing a MAC address) are commonly vulnerable to at least one network exploit." (Reply Br. 4.)

Contrary to Appellants' arguments, the plain language of claim 1 merely requires that "***at least one*** of the nodes" (emphasis added) have an identification assigned "based on a logical assignment grouping ***one or more*** of the plurality of nodes" (emphasis added), and that "each node sharing an

identification" be "commonly vulnerable to at least one network exploit." That is, a single node may have an identification assigned based on a logical assignment which groups that single node alone. In such a case, there is only one node that shares the identification, and that one node is commonly vulnerable to at least one network exploit. In other words, a single node satisfies the plain language of the limitation of claim 1, "at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit."

Holloway teaches multiple managed hubs, where the hubs each run an instance of an intrusion protection system application. (FF 1, 3-4.) Also, as just discussed, a single managed hub meets the recited "at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit" limitation of claim 1. Claim 1 does not require the grouping together of more than one managed hub or the sharing of a MAC address. Thus, Holloway, teaches the "plurality of nodes" limitation as claimed.

Accordingly, we conclude that the Examiner did not err in rejecting claim 1 under 35 U.S.C. § 102(b) as being anticipated by Holloway.

Claims 2-7 were not argued separately, and stand or fall together with claim 1.

With respect to claims 8-10, we agree with Appellants that Holloway does not teach or suggest the limitation of "a network-based intrusion protection system appliance dedicated to filtering inbound and outbound

data frames transmitted across the network medium," as claimed. The Examiner found that the network management station met the "intrusion protection system appliance" limitation. (Answer 5, 7.) But as Appellants correctly point out, there is no indication that the network management station is an intrusion protection system appliance. (Br. 7; Reply Br. 5; *see also* FF 5.) Further, Appellants correctly note that the function of filtering inbound and outbound discovery request frames discussed by the Examiner at page 5 of the Answer is performed by the managed hub rather than by the network management station. (Br. 7, Reply Br. 5; *see also* FF 2-5.) Thus, Holloway does not teach or suggest "a network-based intrusion protection system appliance dedicated to filtering inbound and outbound data frames transmitted across the network medium," as claimed.

Claims 9-10 depend from claim 8, and we find that the Examiner erred in rejecting them for the same reason as discussed with respect to claim 8.

Therefore, we conclude that the Examiner erred in rejecting claims 8-10 under 35 U.S.C. § 102(b) as being anticipated by Holloway.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that:

(1) The Examiner did not err in rejecting claims 1-7 for anticipation under 35 U.S.C. § 102(b).

(2) The Examiner erred in rejecting claims 8-10 for anticipation under 35 U.S.C. § 102(b).

DECISION

The rejection of claims 1-7 for anticipation under 35 U.S.C. § 102(b) is affirmed.

The rejection of claims 8-10 for anticipation under 35 U.S.C. § 102(b) is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

KIS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400